



**AP18:132**

**FOR IMMEDIATE RELEASE**

**AUGUST 23, 2018**

**CONTACT:**

**SOS Press Office**

**(916) 653-6575**

## **Secretary of State Alex Padilla Urges State Political Party Chairs to Take Proactive Steps to Reduce Risk of Cyberattacks**

**SACRAMENTO** - California Secretary of State sent a letter today to the state's political party chairpersons remind them, their party and their party's candidates to be alert and take proactive steps to reduce their risk of being a victim of a cyberattack. The letter was sent in response to recent reports of some political reports being targeted by spear phishing and other attacks.

The full text of the letter can be found below:

August 23, 2018

Dear Party Chairperson:

I write in response to recent media reports regarding the targeting of individual political campaigns — not state election systems — and to remind you, your party, and your party's candidates to be alert and take proactive steps to reduce your risk of being a victim of a cyberattack.

I strongly encourage you, your party, and your party's candidates to take a comprehensive approach to cybersecurity, and follow recognized best practices including, but not limited to, the following:

1. establish and maintain an information security framework that enables your team to detect incidents, investigate effectively, and respond quickly;
2. control access, monitor vendors and contractors as well as employees, and know what your users are doing with your data;
3. monitor user activity;
4. back up your data;
5. beware of social engineering from phone, email or other communications with your users;
6. regularly educate your employees and volunteers on cybersecurity best practices, including how to recognize a phishing email, creating and maintaining strong passwords, utilizing two-factor authentication, and avoiding dangerous applications;

7. make sure your software and hardware security is up to date and properly configured; and
8. run regular security audits, assessments, and penetration testing.

Additionally, the Harvard Kennedy School's Belfer Center for Science and International Affairs published [The Cybersecurity Campaign Playbook](#) in May of this year which you may find useful.

While the Secretary of State's office has no direct authority over an individual candidate's or a political party's campaign infrastructure (cybersecurity or otherwise), I do believe that exploitation of campaign vulnerabilities and the dissemination of misinformation can lead to a lack of confidence by voters in our election process. As such, I encourage you, your party, and your candidates to take cyber threats seriously and take the necessary precautions to minimize your risk. California voters deserve to have confidence in the election information they consume, that their vote matters, and their ballot will be counted and counted as cast.

In the event you do observe or detect any suspicious activity, please alert law enforcement officials immediately and please contact my office with any important information. Also, under a new law now in effect, any journalist, researcher or political campaign that receives voter data from the Secretary of State must inform our office immediately if that information is believed to be compromised.

Thank you for your prompt attention to this matter. Should you have any questions or desire additional information, please feel free to contact Susan Lapsley of my office at (916) 695-1662.

Sincerely,

Alex Padilla  
California Secretary of State

###

**Follow the California Secretary of State on [Twitter](#) and [Facebook](#).**